#2
7-23-01
B. Willard

Docket No. 1359.1041/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Masatoshi SHIOUCHI et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: February 21, 2001

For: VIRTUAL COMMUNICATION CHANNEL AND VIRTUAL PRIVATE COMMUNITY, AND AGENT COLLABORATION SYSTEM AND AGENT COLLABORATION METHOD FOR CONTROLLING THE SAME

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-272195
Filed: September 7, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: February 21, 2001

By: _____

H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ９月 ７日

出 願 番 号
Application Number: 特願２０００－２７２１９５

出 願 人
Applicant (s): 富士通株式会社

２００１年 １月 ５日

特 許 庁 長 官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１０９０１１

【書類名】　特許願

【整理番号】　0095180

【提出日】　平成12年 9月 7日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 13/00

【発明の名称】　仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　塩内　正利

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　岩尾　忠重

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　岡田　誠

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　山崎　重一郎

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　毛利　隆夫

【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　和田　裕二
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　西ヶ谷　岳
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　福田　茂紀
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100095555
【弁理士】
【氏名又は名称】　池内　寛幸
【電話番号】　06-6361-9334
【手数料の表示】
【予納台帳番号】　012162
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9803089
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法

【特許請求の範囲】

【請求項１】　エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、

前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、

前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とするエージェント連携システム。

【請求項２】　前記ポリシーが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含む請求項１に記載のエージェント連携システム。

【請求項３】　エージェント自らが生成したポリシーを他のエージェントに配布し、

前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、

前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する請求項１に記載のエージェント連携システム。

【請求項４】　前記仮想通信路上に認証機構を備え、

前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限・実行条件保持部が保持する権限内容の認証を行う請求項１に記載のエージェント連携システム。

【請求項５】　前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の３つの機関に分かれ、

前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、

前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、

前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行った証明である公開鍵証明書を発行し、

各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てるべき適切な権限内容を指定する請求項４に記載のエージェント連携システム。

【請求項６】　各エージェントが、仮想通信路にログインする際に、前記トラストエンジンを用いて、当該仮想通信路に対応するポリシーの証明書と属性証明書を入力として、ポリシーの証明を得つつログインし、

各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させることを特徴とする請求項１に記載のエージェント連携システム。

【請求項７】　ネットワーク上に存在するエージェント間の情報通信を仲介する方法であって、前記仮想通信路上の各エージェントにおいて、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与し、

前記付与された権限および該権限内容が実行される条件を保持・記憶し、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行し、

前記ポリシーに従って前記仮想通信路を介して各エージェントを連携させるこ

とを特徴とするエージェント連携方法。

【請求項８】　ネットワーク上に存在するエージェント間の情報通信を仲介する処理プログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与する処理ステップと、

前記付与された権限および該権限内容が実行される条件を保持・記憶する処理ステップと、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理ステップと、

各エージェントが前記ポリシーに従って与えられた権限に応じてメッセージをやりとりするように前記仮想通信路を制御する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項９】　ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、

前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ、

前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする仮想通信路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上に存在するエージェントなどコンピュータリソース間においてエージェント連携サービスを提供するエージェント連携装置および方法およびエージェント連携プログラムを格納したコンピュータ読み取り可能な記録媒体に関する。また、必要に応じてエージェント等の間に動的に生成するネッ

トワーク上の仮想的な通信路に関する。

【０００２】

【従来の技術】

近年、コンピュータネットワークが進展し、ネットワーク上に分散した複数のエージェントなどコンピュータリソース間における情報通信サービスが提供されている。従来の技術において、ネットワーク上に存在する複数の通信主体の間を通信路により結ぶ方式として、情報を送信する通信主体が当該情報を受信する通信主体を特定して個別に配信する方式（ピアツーピア接続方式）と、情報を送信する通信主体が当該情報を受信する通信主体を特定することなくネットワーク上に存在する通信主体すべてに対して情報を配信する方式（マルチキャスト方式）がある。

【０００３】

前者のピアツーピア接続方式においても、情報送信において１つの通信主体からメーリングリストなどを用いた同報通信や一斉通信というサービスは可能である。しかし、これは、通信相手のアドレスを指定した１対１の通信が重畳的に行われたものであって、情報送信する通信主体と情報を受信する通信主体との関係でみれば、通信相手を特定して個別に情報を配信するという点において変わらない。

【０００４】

後者の複数の通信主体を接続するマルチキャスト方式としては、ＣＯＲＢＡ（The Common Object Request Broker : Architecture and Specification）のイベントサービス（Event service）やアイピーマルチキャスト（IP-Multicast）、インターネットリレーチャット（Internet Relay Chat : IRC）などが知られている。これら通信サービスは複数のサーバ間で通信を制御するものである。このように複数のサーバを介したエージェント連携サービスの構築のためには複数のサーバを所定のプロトコルで接続・管理する必要があり、それぞれのサーバの実装は、エージェント連携するサービス内容によってチューニングしなければならない。

【０００５】

イベントサービス（Event service）の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。エージェント連携するサービス内容としては、システムのエラー通知が主眼となっており、エラー通知に関するサービスが実装されている。制約としては、メッセージを受信するサーバはデータ受信用のオブジェクトを作成し、特定のトピックに登録しなければならないという制約がある。

【０００６】

アイピーマルチキャスト（IP-Multicast）の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。制約としては、マルチキャストする受信相手のアドレスを予め登録しておかなければならないという制約がある。

【０００７】

インターネットリレーチャット（Internet Relay Chat：IRC）の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。また、エージェント連携するサービス内容としては、ユーザ同士のテキスト通信が主眼である。制約としては、ＩＲＣプロトコルにより通信しなければならないという制約がある。

【０００８】

【発明が解決しようとする課題】

上記従来の技術のピアツーピア接続方式において、メーリングリストなどにより複数のネットワーク上のエージェント等のリソース間の情報通信を行う場合、あらかじめ配信先となる全ての相手のアドレスを登録しておく必要がある。情報配信に際して、情報を配信するエージェント（ユーザ）がすべての配信先を意識的に把握しておく必要が生じることとなる。しかし、情報配信者が必ずしも情報を受信すべき相手を意識的に把握しておくことができない場合もあり、また、多数の配信先を管理することは負担が大きい。広範囲かつ多数の相手に配信するこ

とは非常に困難であり、スケーラビリティに欠けることとなる。さらに、エージェント連携システムが介在するわけではないので、配信の成否についても配信側のエージェントが責任を持つ必要がある。このため、個々のエージェントの負担が非常に大きくなってしまうという問題がある。

【０００９】

上記従来の技術の複数の通信主体を接続するマルチキャスト方式では、以下の問題がある。

【００１０】

まず第１には、ネットワークの配信効率の低下を招くという問題が挙げられる。従来のマルチキャスト方式では、ネットワーク全体に対して情報の受け手を特定することなく配信し、ネットワーク上のエージェント全員が受信することとなる。これは、本来当該情報を受信する必要のないエージェントに対しても情報が毎回送信されることとなり、ネットワーク上に流されるデータ量が大きく、かつ、エージェント側の受信処理量も増大する。

【００１１】

第２には、セキュリティの低下を招くという問題が挙げられる。従来のマルチキャスト方式では、上述したようにネットワーク全体に対して情報の受け手を特定することなく配信し、ネットワーク上のエージェント全員が受信することとなる。そのため本来当該情報を配信すべきでない相手に対しても配信されることとなり、情報の漏洩を防止できない。このように配信経路を制御できないということは即ち情報の到達性の保証に欠けるということでもある。

【００１２】

第３には、システム構成が固定的であり、動的な変更が困難であるという問題がある。従来のマルチキャスト方式では、エージェント連携をサーバが主体となって行うため、仲介する情報の内容や仲介処理内容に応じてサーバが異なるため、構築したシステムの変更が容易ではない。また、複数のサーバおよびエージェント間で情報のやり取りを行い、特定のサービスあるいは問題の解決を行うことを想定したとき、サーバあるいはエージェント間で情報を共有する必要がある。サーバあるいはエージェント間で情報を共有するためには、互いに情報をやり取

りするための通信路が必要であり、複数のサーバやエージェント間で情報交換するためのプログラムを個々のサーバやエージェント側で実装しておく必要が生じる。

【００１３】

上記問題点に鑑み、本発明のエージェント連携システムは、要求やサービス内容に応じて情報を送受信する仮想通信路を柔軟かつ動的に定義付け、制御し、この仮想通信路を用いてエージェント間の連携を実現することを目的とする。この仮想通信路は、エージェント連携サービス開始にあたって動的に定義付け、提供され、エージェント連携サービス内容の変更に伴って動的に更新され、エージェント連携サービスの終了に伴って動的に解消・消滅するものとする。

【００１４】

【課題を解決するための手段】

上記目的を達成するために、本発明のエージェント連携システムは、エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とする。

【００１５】

上記構成により、仮想通信路および仮想通信路上のエージェントが、ポリシーに規定されるエージェントの属性と権限との関係づけに従って動作し、エージェント間の動的な連携を実現することができる。

【００１６】

なお、前記ポリシーは、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェ

ントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含むこととすれば、仮想通信路上のリソース、データの振る舞いをより柔軟に制御することができる。

【００１７】

なお、ポリシーの配布に関しては、エージェント自らが生成したポリシーを他のエージェントに配布し、前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する仕組みとしても良く、また、前記仮想通信路上に前記ポリシーを記憶したポリシーリポジトリを備え、各エージェントが、前記ポリシーリポジトリから必要なポリシーを取り寄せ、前記ポリシー記憶部に記憶する仕組みとしても良い。

【００１８】

また、前記仮想通信路上に認証機構を備え、前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限保持部が保持する権限内容の認証を行うこととすれば、仮想通信路のセキュリティが向上する。例えば、前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の３つの機関に分かれ、前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行った証明である公開鍵証明書を発行し、各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てるべき適切な権限内容を指定する仕組みとしても良い。

【００１９】

このような認証システムを用いることにより、各エージェントが仮想通信路にログインする際に、前記トラストエンジンを用いて当該仮想通信路に対応するポ

リシーの証明書と属性証明書を入力としてポリシーの証明を得つつログインし、各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させるということが可能となる。

【００２０】

なお、前記ポリシー記憶部が前記相互独立に生成・管理している複数のポリシーのうち選択されたポリシーを統合し、統合後のポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に生成したり、前記ポリシーを複数相互独立に分割し、分割後のポリシーごとに、それぞれのポリシーに応じて情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成したりすることができる。

【００２１】

次に、仮想通信路上のエージェント間連携の形態として、他のエージェントに対して要求を出すエージェントは、要求情報の送信にあたり、前記ポリシーに従って要求情報に前記ラベル情報を付して送信し、前記要求情報を受信し、前記要求に対する応答を実行した他のエージェントは、応答情報の送信にあたり、前記ポリシーに従って前記応答情報にラベル情報を付して送信し、前記要求を出したエージェントは、前記ポリシーに従って前記ラベル情報を持つ応答情報を受信するものとすることができ、ラベル情報を用いてエージェント間で要求・応答の連携を行うことができる。

【００２２】

次に、本発明にかかる仮想通信路は、ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ、前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする。

【００２３】

上記の仮想通信路を構築することにより、仮想通信路上のエージェントが、ポ

リシーに規定されるエージェントの属性と権限との関係づけに従って動作するようにエージェント間の動的な連携を与えることができる。

【００２４】

本発明のエージェント連携システムを実現する処理プログラムを記録したコンピュータ読み取り可能な記録媒体を提供すれば、当該記録媒体をコンピュータに読み取ることにより、コンピュータ装置を利用して本発明のエージェント連携システムを構築することができ、エージェント間に仮想通信路を柔軟かつ容易に構築、更新することができるエージェント連携システムを構築できる。

【００２５】

【発明の実施の形態】

以下、本発明のエージェント連携システムの実施形態について、図面を参照しながら説明する。

【００２６】

（実施形態１）

実施形態１のエージェント連携システムは、ネットワーク上のエージェント間の仮想通信路を制御するシステムであって、仮想通信路上の各エージェントが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って各エージェントの属性に応じた権限を持ち、メッセージ受信など権限内容の実行条件が成立した場合に、該当する権限内容を実行することにより、各エージェントを連携させる。本発明の仮想通信路は、上記ポリシーに従って制御され、ポリシーに従ってエージェント同士を仮想的に結び、連携を仲介する。

【００２７】

以下、本発明のエージェント連携システムの実施形態として、最初に本発明におけるポリシー、エージェントの持つ属性に応じて割り当てられる権限（ロール）、データオブジェクトのラベル情報について述べ、エージェント連携システムの装置構成例とその動作例、仮想通信路の動的な生成、変更、消滅の様子を説明する。

【００２８】

まず、本発明におけるポリシー、エージェントの権限（ロール）、データオブジェクトのラベル情報の定義およびそれらの関係について述べる。

【００２９】

ポリシーとは、仮想通信路上におけるエージェントやデータオブジェクトなどのリソースの動作・性質・関係を記述したルールの集合であり、エージェント達の連携により構築される仮想通信路の動作・性質・関係を記述したルールと言える。このようにポリシーとして記述されるルールは多様なものがある。例えば、エージェントが持つ属性と、それら属性に対応して割り当てられる仮想通信路上での操作や動作などに関する権限の集合（ロール）の関係を記述したルールがある。また、データオブジェクトが持つ属性と、それら属性に対応して割り当てられる仮想通信路上でのエージェントからの操作等に対応する反応の集合（ラベル）との関係を記述したルールがある。また、上記したエージェントの持つ権限の集合（ロール）とデータオブジェクトの反応の集合（ラベル）の間の関係を記述したルールがある。また、上記したエージェントの持つ権限の集合（ロール）と権限の集合（ロール）同士の関係を記述したルールもある。さらに、本発明の仮想通信路自体、参加するエージェント達自身のネットワークで構成されているので、仮想通信路の生成・変更・消滅に関してもエージェントの動作の一環として記述することができる。このように、ポリシーには仮想通信路の生成・変更・消滅を含む仮想通信路そのものの動作に関するルールも含まれる。

【００３０】

なお、このポリシーは、後述する他の実施形態４に示すようにポリシーリポジトリサーバというポリシーを集中的に管理するサーバをネットワーク上に用意して管理し、各エージェントが取り寄せる仕組みでも良く、また、各エージェント自らが生成・証明したポリシーをネットワーク上に配布し、当該ポリシーを受け取り（契約し）、当該ポリシーに従ってロールを得たエージェント間で仮想通信路を形成する仕組みとしても良い。後者は仮想通信路を用いた完全自立分散型のエージェント連携と言える。例えば、エージェント自らが管理する画像データベースのコンテンツ配布をサービスしたいエージェントが、一定の料金を支払うという契約を結んだエージェントであるという属性と、該画像データベースコンテ

ンツをダウンロードするという権限との関係を記述したルールをポリシーとし、該ポリシーをネットワーク上に配布するなどという利用が想定できる。

【００３１】

ポリシーの実例を図１に示す。図１は、ポリシー記述の一例を示す図である。簡単な画像イメージ配送サービスに関するポリシー例を示した。１は、ポリシーとして配布されるべきファイルなどを記述している。ここで、“image.jar”はロール（権限内容）を実行するプログラムモジュールであるロールプログラムファイル、“image.xml”は本ポリシー記述ファイルを指している。２は、ロール割り当てのためのルール群である。まず最初にロール割り当てのための条件、即ち、属性とその値の指定（図中３）を記述し、続いてそれが満たされた場合に割り当てられるロールが記述される（図中４）。図１のポリシーの例では、まず登録料の支払いについて属性に注目し、登録料を支払っていれば登録ユーザのロール（権限内容）が与えられる。逆に支払っていない場合はルールの第３項目に定義されているように未登録ユーザ用のロール（権限内容）が与えられる。また、画像イメージコンテンツの提供者になるかどうかの契約に着目すると、契約を行った場合には画像イメージコンテンツの提供者としてのロール（権限内容）が与えられる。このようなポリシー記述を持つポリシーを用意し、各エージェントが装備することにより、ポリシー記述に従って制御される仮想通信路を生成することができる。

【００３２】

なお、エージェントのロールとは、上記にも述べたように、エージェントの属性に応じて割り当てられた権限の集合である。エージェントは付与された権限に応じて動作し、動作の一環として他のエージェントとの連携処理を実行する。ロールには実行できる権限内容が決められており、また、当該権限内容を実行するための実行条件が決められている。ここで実行条件とは、例えば、仮想通信路から特定のメッセージを受信することや、エージェントのステータスが特定の状態になったことや、あるイベントが起こった場合、あるイベントから一定時間が経過した場合など多様な条件がある。

【００３３】

データオブジェクトのラベル情報とは、上記にも述べたように、データオブジェクトの属性に対応して割り当てられるエージェントからの操作等に対応する反応の集合である。例えば、一定権限を持つエージェントからのデータ内容の読み出し操作、書き込み操作、削除操作を認めることや、一定権限を持つエージェントによる演算操作、検索操作、転送操作を認めることなどがある。

【００３４】

次に、エージェント連携システムの装置構成例について説明する。

【００３５】

図２は、エージェント連携システムの装置構成例を模式的に示す図であり、一つのエージェントの内部構成例を示した。本発明のエージェント連携システムは、図２に示した構成を持つ複数のエージェントがネットワークを介して連携し合うシステムであり、本発明の仮想通信路は、これらエージェント間を結ぶネットワーク上に仮想的に形成される連携の場、コミュニケーションの場と言える。

【００３６】

図２において、１００はエージェントであり、２００は外部ネットワーク、２１０は内部フィールドである。１０はエージェントネットワークコネクタ、２０はセキュリティマネジャ、３０はロールマネジャ、４０は属性マネジャ、５０はロールプログラムデータベース、６０はフィールドコネクタ、７０はロールメソッドテーブル、８０はロール実行部である。

【００３７】

上記のエージェント１００の構成において、セキュリティマネジャ２０、ロールマネジャ３０、属性マネジャ４０、ロールプログラムデータベース５０は、ポリシーに従って内部フィールド２１０の生成、変更、消滅を実行するためのモジュールである。また、上記エージェント１００は、フィールドコネクタ６０を持っている。セキュリティマネジャ２０はフィールドコネクタ６０上に内部フィールド２１０を構築する。さらに、ロールマネジャ３０、属性マネジャ４０が内部フィールド２１０につながるロールメソッドテーブル７０、ロール実行部８０をそれぞれ構成する。図２の例では３つの内部フィールド２１０ａ～ｃ、ロールメソッドテーブル７０ａ～ｃ、ロール実行部８０ａ～ｃが構築されている。

【００３８】

なお、内部フィールド２１０、ロールメソッドテーブル７０、ロール実行部８０は、権限実行条件が成立した場合に権限内容（アクション）の実行を行うためのモジュールである。例えば外部ネットワーク２００から特定のメッセージを受信したことを条件として対応するロールを反応させ、実行する。

【００３９】

各モジュールを説明する。

【００４０】

ネットワークエージェントコネクタ１０は、エージェント１００と外部ネットワーク２１０とを接続する通信インタフェースを提供する部分である。メッセージを外部ネットワーク２００から受け取り、メッセージの種類に応じて該メッセージをセキュリティマネジャ２０に渡すかフィールドコネクタ６０に渡すかを振り分ける。受け取ったメッセージが、フィールド生成メッセージやフィールド検索メッセージやフィールド削除メッセージなどフィールドの生成、変更、消滅に関わるメッセージであればセキュリティマネジャ２０に振り分け、メッセージがエージェント連携に関するフィールドメッセージであればフィールドコネクタ６０に振り分ける。

【００４１】

セキュリティマネジャ２０は、フィールドの生成、変更、消滅に関わるメッセージを受け取ると該メッセージの正当性を確認する機能と、該メッセージ内容を解釈し、フィールドの生成、変更、消滅の指示に応じて内部フィールド２１０の生成、変更、消滅を実行する機能と、該メッセージからポリシーを抽出する機能を有する。メッセージの正当性を確認する機能は本発明のエージェント連携システムのセキュリティ向上のために必要な機能である。内部フィールド２１０の生成、変更、消滅を実行する機能に関しては、フィールドコネクタ６０は生成された内部フィールド２１０と外部ネットワーク２００を接続するポイントとなるものであり、その生成、変更、消滅は、セキュリティマネジャ２０が実行することとしている。なお、メッセージからポリシーを抽出する機能により図１に示されたようなポリシーが抽出され、ロールマネジャ３０に渡される。

【００４２】

ロールマネジャ３０は、セキュリティマネジャ３０から受け取ったポリシーを解釈し、エージェントが持つ属性と照合を行い、ロール生成、消滅を制御する。ポリシーの中の各ルールの条件部に指定された属性とその値と、エージェントが持つ属性とその値を参照するため、属性マネジャ４０に対して属性とその値を問い合わせを行う。属性マネジャ４０からの回答を得て、ルールの条件を満足する場合にはロールメソッドテーブル７０に対してロール名を通知し、ロールメソッドテーブル７０の構築、内容の変更を指示する。なお、ロールマネジャ３０はポリシーを記憶しておくポリシー記憶部３１を備え、ポリシーを格納しておく。

【００４３】

属性マネジャ４０は、属性データベース４１を備えている。属性マネジャ４０は、ロールマネジャ３０からのエージェントが持つ属性とその値の問い合わせに対して、属性データベース４１を参照して該問い合わせに対して回答する。

【００４４】

ロールプログラムデータベース５０は、ロール実行部８０を構築するためのプログラムを格納したデータベースであり、ロール実行部８０の構築時にロールマネジャ３０の制御により必要なプログラムが取り出され、ロール実行部８０の構築に供される。なお、このロールプログラムは、ネットワークを介した外部に存在するものであっても良く、必要に応じてアクセスし、ロールプログラムをダウンロードできる仕組みであれば良い。

【００４５】

内部フィールド２１０は、その生成、変更、消滅に関しては、セキュリティマネジャ２０からの指示により生成、変更、消滅される。内部フィールド２１０の生成指示があれば、フィールドコネクタ６０上に新しい内部フィールドが生成される。同様に存在している内部フィールド２１０の消滅指示があれば、フィールドコネクタ６０が内部フィールド２１０を消滅させる。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、まず、フィールドコネクタ６０は、エージェントネットワークコネクタ１０からフィールドメッセージを受け、フィールドメッセージの内容や属性を調べ、適切なフィールドコネ

クタ６０のみが内部フィールド２１０に対して当該メッセージを流す。また、ロール実行部８０の実行処理の一環として返される応答メッセージなどを受け、該応答メッセージをエージェントネットワークコネクタ１０を介して外部ネットワーク２００に対して発信する。

【００４６】

ロールメソッドテーブル７０は、ロールマネジャ３０からの指示を受け、テーブルの構築、その内容の変更を行う。内部フィールドの生成に際しては、ロールマネジャ３０からロール名の通知を受けて、ロールプログラム集より適切なロールを呼び出し、指定されたロールに応じたメソッドを関係づけて格納する。また、当該ロールが起動されるための実行条件を関係づけてテーブルに格納しておく。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、フィールドメッセージの受信や、各種イベントの発生、エージェントステータスの変更などの条件を検知したフィールドコネクタ６０から、該条件を実行条件に持っているロールがあるか否かの問い合わせを受け、該当するロールがある場合にはそのロールを制御するメソッドを指定し、フィールドコネクタ６０に通知する。

【００４７】

次に、ロール実行部８０は、ロールマネジャ３０からの指示を受け、ロールプログラムデータベース５０から適切なロールを呼び出して、格納しておく。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、フィールドメッセージに従い、フィールドコネクタ６０により特定のメソッドが起動されると該メソッドに対応するロール内容を実行する。逆に、実行条件が成り立たなくなれば、該メソッド制御のもと対応するロール実行が停止される。

【００４８】

以上に示した構成例のエージェント連携システムの動作を図３のフローチャートを参照しつつ説明する。以下の例では、ロール実行条件として特定のフィールドメッセージを受信することをロールの実行条件とした例を説明する。なお、図３のフローチャートにおいて説明の便宜上、エージェントネットワークコネクタをＡＮＣ、フィールドコネクタをＦＣ、セキュリティマネジャをＳＭ、ロールマ

ネジャをＲＭ、属性マネジャをＡＭと記号で略記した。

【００４９】

まず、エージェントネットワークコネクタ１０が外部ネットワーク２００をモニタし、データ受信を待っている（ステップＳ３０１）。

【００５０】

外部ネットワーク２００からデータを受信すると（ステップＳ３０１：Ｙ）、エージェントネットワークコネクタ１０は、該データがフィールドメッセージか否かをチェックする（ステップＳ３０２）。

【００５１】

該データがフィールドメッセージである場合（ステップＳ３０２：Ｙ）、エージェントネットワークコネクタ１０は、フィールドメッセージからフィールド名を取り出し、該当するフィールドコネクタ６０へ転送する（ステップＳ３０３）。

【００５２】

フィールドコネクタ６０は、ロールメソッドテーブル７０を参照し、該メッセージ受信を実行条件としているロールを検索する（ステップＳ３０４）。対応するロールが存在する場合（ステップＳ３０４：Ｙ）は、該ロールの実行を制御するメソッドが起動され、ロールが実行され（ステップＳ３０５）、ステップＳ３０１に戻る。対応するロールが存在しない場合（ステップＳ３０４：Ｎ）、ロールは何も反応せず実行されずステップＳ３０１に戻る。

【００５３】

次に、ステップＳ３０２において、受信データがフィールドメッセージでない場合（ステップＳ３０２：Ｎ）、エージェントネットワークコネクタ１０は、データをセキュリティマネジャ２０に転送し、セキュリティマネジャ２０は受信データが新しいフィールド生成メッセージであるか否かをチェックする（ステップＳ３０６）。

【００５４】

受信データが新しいフィールド生成メッセージである場合（ステップＳ３０６：Ｙ）、セキュリティマネジャ２０は、受信メッセージからポリシーを取り出し

、ロールマネジャ３０へ転送する（ステップＳ３０７）。ロールマネジャ３０はポリシーに記述されている属性およびその値に関し、属性マネジャ４０に問い合わせ、属性マネジャ４０からの応答結果からエージェントに与えられるロールを決定する（ステップＳ３０８）

ロールマネジャ３０は、フィールド生成メッセージに対応して、フィールドコネクタ６０を生成し、該フィールドコネクタに構築すべきロール名とその内容を通知する（ステップＳ３０９）。ロールマネジャ３０は、通知されたロール内容を構築するため、ロールプログラム集から該当するロールをロール実行部８０にロードし、必要なロール実行モジュールを構築し、内部フィールド２１０を生成する（ステップＳ３１０）。このように内部フィールド２１０が生成されれば、適切にステップＳ３０１に戻る。

【００５５】

次に、ステップＳ３０６において、受信データが新しいフィールド生成メッセージでない場合（ステップＳ３０６：Ｎ）、受信データがフィールド検索メッセージであるか否かをチェックする（ステップＳ３１１）。受信データがフィールド検索メッセージである場合（ステップＳ３１１：Ｙ）、セキュリティマネジャ２０はメッセージ内容からフィールド検索条件を抽出し、検索条件に該当するフィールド名をエージェントネットワークコネクタ１０を介して検索元に対して返信する（ステップＳ３１２）。返信後、適切にステップＳ３０１に戻る。

【００５６】

受信データがフィールド検索メッセージでない場合（ステップＳ３１１：Ｎ）、セキュリティマネジャ２０は、受信メッセージがフィールド削除メッセージであるか否かをチェックする（ステップＳ３１３）。受信メッセージがフィールド削除メッセージである場合（ステップＳ３１３：Ｙ）、セキュリティマネジャ２０は、フィールド削除メッセージから削除すべきフィールド名を抽出し、該当するフィールドのフィールドコネクタ６０に対してフィールドの削除を通知する（ステップＳ３１４）。フィールドの削除を通知されたフィールドコネクタ６０は、管理する内部フィールド２１０を削除する（ステップＳ３１５）。なお、内部フィールド２１０の消滅に伴って対応するロールメソッドテーブル７０、ロール

実行部８０が消滅する。フィールド削除後、適切にステップＳ３０１に戻る。

【００５７】

受信メッセージがフィールド削除メッセージでない場合（ステップＳ３１３：Ｎ）、この例では、受信データに対する有効な応答が行われず、ステップＳ３０１に戻って、次のデータ受信を待つ。

【００５８】

以上が、本実施形態１のエージェント連携システムによる仮想通信路の生成、変更、消滅、生成された仮想通信路を用いたエージェント連携動作の流れの一例である。

【００５９】

本実施形態１のエージェント連携システムは、以上に見たように、本発明のエージェント連携システムおよびエージェント間を結ぶ仮想通信路は、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、ポリシーに従ってポリシーに従ってエージェント同士を仮想的に結び、エージェント間の連携を仲介できる。

【００６０】

（実施形態２）

実施形態２では、本発明のエージェント連携システムにおいて、エージェント間の連携の形態ついてバリエーションを持たせるように仮想通信路を定義付け、制御することができることを説明する。

【００６１】

なお、エージェント連携システムの装置構成例は図２で示したものと同様であるのでここでの説明は省略する。

【００６２】

第１に、本発明のエージェント連携システムにおいて、エージェント間の連携を複数相互独立な形態で構築することが可能である。この場合、セキュリティマネジャ２０、ロールマネジャ３０が、ポリシーに従い、複数相互独立の内部フィールド２１０を生成・管理し、ロール実行により各エージェントが連携することにより、複数相互独立のエージェント連携関係が仮想通信路上に構築される。こ

の複数相互のエージェント間連携の構築の様子を概念的に示したものが図４（ａ）である。

【００６３】

第２に、本発明のエージェント連携システムにおいて、複数相互独立な形態で構築されているエージェント間の連携を統合することが可能である。この場合、セキュリティマネジャ２０、ロールマネジャ３０が相互独立に生成・管理している複数の内部フィールド２１０のうち選択したものを統合する指示を出すことにより、対応するフィールドコネクタが１つのフィールドコネクタとして再生成され、内部フィールドも１つのものが再生成され、既存の２つの相互独立のエージェント間連携を統合した形のエージェント間の連携が生成される。この複数相互のエージェント間連携を統合する様子を概念的に示したものが図４（ｂ）である。

【００６４】

第３に、本発明のエージェント連携システムにおいて、既存のエージェント間の連携を分割することが可能である。この場合、セキュリティマネジャ２０、ロールマネジャ３０が、分割後の一方のフィールドと他方のフィールドのそれぞれの生成指示を出すことにより、対応するそれぞれのフィールドコネクタが生成され、それぞれの内部フィールドも生成される。このエージェント間連携を分割する様子を概念的に示したものが図４（ｃ）である。

【００６５】

第４に、本発明のエージェント連携システムにおいて、エージェント間連携を親として、いわゆる入れ子状態で、子に相当するエージェント連携を構築することも可能である。この場合、セキュリティマネジャ２０、ロールマネジャ３０が、親のフィールド生成指示と子のフィールド生成指示を出し、親フィールドと子フィールドが生成される。このエージェント間連携の入れ子状態の様子を概念的に示したものが図４（ｄ）である。

【００６６】

以上に示すように、本発明のエージェント連携システムは、ポリシーに従って構築するエージェント間の連携の形態ついてバリエーションを持たせることがで

きる。

【００６７】

（実施形態３）

実施形態３のエージェント連携システムとして、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証、完全自立分散構成の場合におけるログインの連鎖による安全なポリシー配布、不正アクセスに対する処理、エージェント連携の確認などに関し、セキュリティ向上を図った構成例を示す。

【００６８】

まず、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証を説明し、各エージェントにおいて、証明された真正なポリシーを受け、正しく保証されたロールが割り当てられ、仮想通信路に参加する仕組みを説明する。

【００６９】

図５は、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証を行う概念を模式的に示した図である。図５において、５は、ポリシー証明書の発行主体となる権威機関であるポリシー管理機関（policy approving authority：ＰＡＡ）、６は、属性証明書の発行主体となる権威機関である属性管理機関（attribute authority：ＡＡ）、７は、個体認証を行い、公開鍵証明書の発行主体となる権威機関である個体認証機関（certification authority：ＣＡ）である。このように３つの権威機関を設けることにより、ポリシー認証、属性認証、個体認証という３つの側面についてそれぞれ異なる権威機能を分散して設け、広域分散環境などにおける仮想通信路の構築、仮想通信路を用いた情報のやり取りについて高いセキュリティを持たせることを狙っている。

【００７０】

ここで、ポリシー証明書とは、ポリシーを記述したデータに対して電子署名を付したものである。つまりネットワークに正当に配布された真正のポリシーであることが認証されているものである。このポリシー証明書は、ネットワークを介してエージェントなどに配布される。あるポリシー証明書によって同一のポリシ

ーが伝播している仮想的なネットワーク領域が信用ドメインとなり、仮想通信路によって形成されるコミュニケーション空間とも言える。新しいエージェントがある信用ドメインに加わり仮想通信路に参加しようとする場合にはまず、対応するポリシー証明書を受け取り、その内容に合意してポリシー証明書に基づいた権限割り当てを受ける必要がある。

【００７１】

属性証明書とは、個人の属性を認証する属性管理機関６が、各エージェントが持っている属性を証明したものを言う。例えば、ＩＴＵ－ＴＸ．５０９属性証明書に準じた形で記述される。なお、属性管理機関６による属性証明書の発行にあたっては、図２に示した各エージェントが持つ属性管理データベース５０に対してアクセスし、各エージェントが持っている属性を参照することができる。

【００７２】

公開鍵証明書とは、ネットワーク上における本人認証を行うものであって、個体認証を行う権威機関である個体認証機関７により、例えば、ＩＴＵ－ＴＸ．５０９公開鍵証明書などの公開鍵認証基盤に基づいて発行される。

【００７３】

次に、各エージェントにおいて、証明された真正なポリシーを受け、正しく保証されたロールが割り当てられる仕組みを説明する。

【００７４】

図５において、８は、各エージェントが実装するトラストエンジンであって、ネットワーク上で伝播されているポリシー証明書や属性証明書を入力として解釈し、それらポリシー証明書や属性証明書に対応した適切なロールを特定して割り当てるものである。なお、この各エージェントが実装するトラストエンジンは、実施形態１で図２を用いて説明した各エージェント構成において、ロールマネジャ３０および属性マネジャ４０による複合機能として構成される。

【００７５】

本実施形態３の認証システムでは、各エージェントがこのトラストエンジン８を実装し、ポリシー管理機関５、属性管理機関６、個体認証機関７を信頼し、発行されているポリシー証明書や属性証明書をトラストエンジン８により安全に解

釈し、ロールの割り当てを実行する。この割り当てられたロールにはロール保証書が付され、ロールの正当性が保証される。なお、トラストエンジン自体の正当性は、例えば、公開鍵認証基盤に基づく、ＳＳＬによる相互認証とオブジェクト署名の検証によって証明でき、従ってこのトラストエンジンにより生成されたロール保証書の正当性も保証される。

【００７６】

このように生成されたロール保証書に基づいて、各エージェントにおいて、ロールマネジャの制御のもと、ロールが割り当てが実行される。

【００７７】

以上の認証システムに基づいて、ポリシー証明、ロール保証が実行され、高いセキュリティのもと、仮想通信路が生成・制御され、各エージェントが該仮想通信路に安全に出入りできる。

【００７８】

次に、完全自立分散構成の場合におけるログインの連鎖による安全なポリシー配布について説明する。同一のポリシーが伝播している仮想通信路上の参加エージェントは任意に出入りが可能でありその参加者は動的に変化しうる。本発明の仮想通信路を制御するエージェント連携システムを分散型システムとして構築した場合には、真正が保証された集中管理用の特定のエージェントが存在しないので、新しく仮想通信路に参加しようとするエージェントは、既に参加済みの任意のエージェントに対してログインの要求を行うこととなる。各エージェントによる仮想通信路へのログインは、上記図５に見たように、各エージェントが持つ属性情報とポリシーに基づいて行われ、ログインの結果としてエージェントにはロールが割り当てられる。ここで、ログイン時にロール割り当て処理を行うトラストエンジン８は、既に信用ドメインに参加しているエージェントに稼動しているものではなく、新規に参加しようとしているエージェント側で稼動しているものを使用することがポイントとなる。これにより、一種のプライバシー情報と言える属性情報を他に通知することなく、かつ、仮想通信路全体のセキュリティを低下させることなく安全にログイン処理を行うことができる。このような個々のエージェントのログインの連鎖によって、集中管理システムなしにログインを介し

てポリシーを安全に伝播させることができ、各エージェントは仮想通信路に対して任意にログイン、ログアウトすることができる。

【００７９】

次に、不正アクセスや、参加者からの要望に応じて仮想通信路を消滅させる処理について説明する。これは、エージェント間でメッセージが所定通りにやり取りされ、連携が正常に実行されているか、さらに、不正なアクセスがないかについてチェックし、不正なアクセスがあった場合に動的に仮想通信路を無効化するものである。図６は、エージェント間でのメッセージのやり取りの確認、不正アクセス検知を実行するエージェント連携システムの構成例を示す図である。実施形態１で説明した図２の構成と同様の部分についてはここでは説明を省略する。

【００８０】

図６に示すように、エージェント１００ａは、エージェント連携確認部９０を備えている。また、各エージェントは処理機能の一つとしてメッセージを受信した場合に受領通知を仮想通信路上に返す仕組みとする。エージェント連携確認部９０は、エージェントネットワークコネクタ１０を介して仮想通信路上に送信されているメッセージをモニタし、あるエージェントから流された依頼メッセージを確認する。その後、モニタを続け、当該依頼メッセージを受領した他のエージェントから当該依頼メッセージを受信した旨の受領通知メッセージをモニタして依頼メッセージの受信を確認する。このように、エージェント連携確認部９０を用いて仮想通信路上で送信されたメッセージとそのメッセージに対する受領通知をモニタすることにより、エージェント間の情報の仲介が正常に実行され、エージェントの連携が正常に実行されていることを確認する。

【００８１】

エージェントネットワークコネクタ１０は、アクセス権管理部１１と不正アクセス検知部１２を備えている。

【００８２】

不正アクセス検知部１２は、仮想通信路に対する不正アクセスを検知する部分である。不正を検知する方法は種々あるが、例えば、アクセス権管理部１１が管理しているアクセス権の内容に違反してエージェントがアクセスし、メッセージ

を送受信していれば、不正アクセス検知部１２は、不正アクセスがあったことを検知する。また、例えば、不正アクセス検知部１２は、メッセージの改ざんを検知する機能を有している。電子署名がメッセージに埋め込まれている場合に電子署名が壊れていないかチェックしたり、電子透かしが埋め込まれている場合に電子透かしに異常が見られないかチェックしたり、ロールに相応しくないメッセージを受信したことをチェックしたり、データオブジェクトがアクセスしてきたエージェントの資格に合わないメソッドでアクセスされていないかチェックしたりすることにより不正アクセスを検知する。

【００８３】

不正アクセス検知部１２は不正アクセスを検知すれば、セキュリティマネジャ２０にフィールドの消滅指示を通知し、セキュリティマネジャ２０が不正アクセスが試みられた内部フィールドを消滅させ、外部ネットワーク２００との接続を遮断する。

【００８４】

なお、上記の仮想通信路の消滅は、自発的にエージェント側からも請求しうる構成とすることができる。例えば、ロール実行部８０のロールなどが仮想通信路を消滅させたい旨の要求を出した場合、フィールドコネクタ６０を介してエージェントネットワークコネクタ１０に通知され、エージェントネットワークコネクタ１０がセキュリティマネジャ２０に対して該当する仮想通信路の消滅指示を出す。セキュリティマネジャ２０は対応する内部フィールドを消滅させる。

【００８５】

また、仮想通信路に対して有効期限を設けておき、仮想通信路を消滅させることもできる。例えば、セキュリティマネジャ２０またはフィールドコネクタ６０がタイマを備え、タイマにより有効期限に到達したか否かを検知し、有効期限の経過が検知されればセキュリティマネジャ２０の消滅指示を受けて対応する内部フィールド２１０が消滅され、または、有効期限に到達したことを検知したフィールドコネクタ６０が自動的に該当する内部フィールド２１０を消滅させる。

【００８６】

また、本発明のエージェント連携システムはエージェント間でやりとりするメ

ッセージを暗号化することによりセキュリティを向上することも可能である。相互に送信メッセージの暗号化処理機能と、受信メッセージの復号化処理機能を有し、メッセージの送受信にあたりメッセージの暗号化復号化処理を実行する。どの暗号鍵、復号鍵を用いるかについては、例えば、用いられるロールに基づいて決定することができる。

【００８７】

以上、実施形態３のエージェント連携システムは、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証、エージェント間連携でのメッセージのやり取りの暗号復号化、各エージェントによる仮想通信路へのアクセス権の管理、不正アクセスに対する処理、エージェント連携の確認などに関し、セキュリティ向上を図ることができる。

【００８８】

（実施形態４）

実施形態４のエージェント連携システムは、ポリシーの頒布に関し、ポリシーリポジトリサーバを備えたものである。

【００８９】

図７は、本実施形態４にかかるポリシーリポジトリサーバを備えたエージェント連携システムの構成例である。３００は、ポリシーリポジトリサーバであり、複数のポリシーが格納されている。

【００９０】

エージェント１００が仮想通信路を構築または既存の仮想通信路に参加する場合、エージェントは対象となる仮想通信路を記述したポリシーを得て、当該ポリシーに従ってロールを構築しなければならない。エージェント１００はポリシーリポジトリサーバ３００にアクセスし、対象となるポリシーの送信を依頼する。ポリシーリポジトリサーバ３００は、格納しているポリシーから該当するポリシーを依頼元のエージェント１００に送信する。ポリシーの頒布を受けたエージェント１００は、エージェントネットワーク１０を介してセキュリティマネジャ２０に渡され、セキュリティマネジャ２０がポリシーを抽出し、ロールマネジャ３０にポリシーを渡し、ロールマネジャ３０はポリシーをポリシー記憶部３１に格

納する。セキュリティマネジャ２０およびロールマネジャ３０が、受け取ったポリシーに従って該当する内部フィールドを構築する点については実施形態１と同様である。

【００９１】

以上、本発明のエージェント連携システムは、ポリシーを一元的に管理し、頒布するポリシーリポジトリサーバを備え、未だポリシーを持っていないエージェントに対するポリシーの頒布を実行でき、また、ポリシーそのものの更新がある場合においてエージェントに対して更新後のポリシーを頒布することができる。

【００９２】

（実施形態５）

本発明のオブジェクトエージェント連携システムは、上記に説明した構成を実現する処理ステップを記述したプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することにより、各種コンピュータを用いて構築することができる。本発明のオブジェクトエージェント連携システムを実現する処理ステップを備えたプログラムを記録した記録媒体は、図８に図示した記録媒体の例に示すように、ＣＤ－ＲＯＭ１００２やフレキシブルディスク１００３等の可搬型記録媒体１００１だけでなく、ネットワーク上にある記録装置内の記録媒体１０００や、コンピュータのハードディスクやＲＡＭ等の記録媒体１００５のいずれであっても良く、プログラム実行時には、プログラムはコンピュータ１００４上にローディングされ、主メモリ上で実行される。

【００９３】

さらに、ソースプログラムをコンパイルしたもののみならず、いわゆるネットワークを介してクライアントコンピュータに中間言語形式のアプレットを送信し、クライアントコンピュータ上でインタープリタ実行して動作する構成であっても良い。

【００９４】

本発明の仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法において、さらに以下の項を開示する。

【００９５】

（付記１）エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、

前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、

前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とするエージェント連携システム（１）。

【００９６】

（付記２）前記ポリシーが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含む付記１に記載のエージェント連携システム（２）。

【００９７】

（付記３）各エージェントにおいて、前記ポリシー記憶部に記憶されているポリシーの内容を更新し、前記ルールの消去、変更、新たなルールの追加を行うことができる付記１に記載のエージェント連携システム。

【００９８】

（付記４）前記処理実行部が予め処理機能モジュールを保持し、前記権限保持部が保持する権限内容に沿って、前記処理実行部に含まれる処理機能モジュールを選択的に有効化して処理機能を構築する付記１に記載のエージェント連携システム。

【００９９】

（付記５）前記処理実行部における処理機能の構築において、前記権限内容の

実行に必要な処理機能モジュールが予め保持されていない場合、前記仮想通信路を介してネットワーク上のリソースから必要な処理機能モジュールを受信して利用する付記４に記載のエージェント連携システム。

【０１００】

（付記６）エージェント自らが生成したポリシーを他のエージェントに配布し、

前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、

前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する付記１に記載のエージェント連携システム（３）。

【０１０１】

（付記７）前記仮想通信路上に前記ポリシーを記憶したポリシーリポジトリを備え、

各エージェントが、前記ポリシーリポジトリから必要なポリシーを取り寄せ、前記ポリシー記憶部に記憶する付記１に記載のエージェント連携システム。

【０１０２】

（付記８）前記仮想通信路上に認証機構を備え、

前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限・実行条件保持部が保持する権限内容の認証を行う請求項１に記載のエージェント連携システム（４）。

【０１０３】

（付記９）前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の３つの機関に分かれ、

前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、

前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、

前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行

った証明である公開鍵証明書を発行し、

各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てるべき適切な権限内容を指定する付記８に記載のエージェント連携システム（５）。

【０１０４】

（付記１０）各エージェントが、前記仮想通信路への参加・不参加を自ら選択できる付記１に記載のエージェント連携システム。

【０１０５】

（付記１１）各エージェントが、仮想通信路にログインする際に、前記トラストエンジンを用いて、当該仮想通信路に対応するポリシーの証明書と属性証明書を入力として、ポリシーの証明を得つつログインし、

各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させることを特徴とする付記９に記載のエージェント連携システム（６）。

【０１０６】

（付記１２）前記ポリシー記憶部が、相互独立のポリシーを複数生成・管理し、それらポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成した付記１に記載のエージェント連携システム。

【０１０７】

（付記１３）前記ポリシー記憶部が前記相互独立に生成・管理している複数のポリシーのうち選択されたポリシーを統合し、統合後のポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に生成する付記１に記載のエージェント連携システム。

【０１０８】

（付記１４）前記ポリシー記憶部が、前記ポリシーを複数相互独立に分割し、分割後のポリシーごとに、それぞれのポリシーに応じて情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成する付記１に記載のエージェント連携システム。

【０１０９】

（付記１５）前記ポリシー記憶部は、第１のポリシーと、前記第１のポリシーに属し、前記第１のポリシーに対して新たなルールを追加した第２のポリシーを記憶し、前記第１のポリシーに応じたエージェント間の連携上に前記第２のポリシーに応じたエージェント間の連携を生成した付記１に記載のエージェント連携システム。

【０１１０】

（付記１６）他のエージェントに対して要求を出すエージェントは、要求情報の送信にあたり、前記ポリシーに従って要求情報に前記ラベル情報を付して送信し、

前記要求情報を受信し、前記要求に対する応答を実行した他のエージェントは、応答情報の送信にあたり、前記ポリシーに従って前記応答情報にラベル情報を付して送信し、

前記要求を出したエージェントは、前記ポリシーに従って前記ラベル情報を持つ応答情報を受信する付記１に記載のエージェント連携装置。

【０１１１】

（付記１７）前記権限保持部において保持されている権限が有効期限を持ち、有効期限の経過により該権限を無効化する付記１に記載のエージェント連携システム。

【０１１２】

（付記１８）前記ラベル情報が有効期限を持ち、有効期限の経過により各エージェントにおいて該ラベル情報の付されたメッセージを無視する付記１に記載のエージェント連携システム。

【０１１３】

（付記１９）前記仮想通信路が有効期限を持ち、有効期限の経過により該仮想通信路が消滅する付記１に記載のエージェント連携システム。

【０１１４】

（付記２０）前記仮想通信路上または前記エージェントに、前記仮想通信路に対する不正アクセスを検知する不正アクセス検知部を備え、

前記不正アクセス検知部により前記仮想通信路への不正アクセスを検知したことを契機として、各エージェントが前記仮想通信路への接続を断ち、前記仮想通信路を動的に消滅する付記１に記載のエージェント連携システム。

【０１１５】

（付記２１）前記仮想通信路上のいずれかのエージェントからの仮想通信路の消滅要求を受け、各エージェントが前記仮想通信路への接続を断ち、前記仮想通信路を動的に消滅させる付記１に記載のエージェント連携システム。

【０１１６】

（付記２２）ネットワーク上に存在するエージェント間の情報通信を仲介する方法であって、前記仮想通信路上の各エージェントにおいて、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与し、

前記付与された権限および該権限内容が実行される条件を保持・記憶し、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行し、

前記ポリシーに従って前記仮想通信路を介して各エージェントを連携させることを特徴とするエージェント連携方法（７）。

【０１１７】

（付記２３）ネットワーク上に存在するエージェント間の情報通信を仲介する処理プログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与する処理ステップと、

前記付与された権限および該権限内容が実行される条件を保持・記憶する処理ステップと、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理ステップと、

各エージェントが前記ポリシーに従って与えられた権限に応じてメッセージをやりとりするように前記仮想通信路を制御する処理ステップとを備えた処理プロ

グラムを記録したことを特徴とする記録媒体（８）。

【０１１８】

（付記２４）ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、

前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ、

前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする仮想通信路（９）。

【０１１９】

【発明の効果】

本発明のエージェント連携システムおよびエージェント間を結ぶ仮想通信路によれば、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、ポリシーに従ってポリシーに従ってエージェント同士を仮想的に結び、エージェント間の連携を仲介できる。

【０１２０】

本発明のエージェント連携システムは、ポリシーに基づいて、エージェント間の多様な連携形態を柔軟に構築・変更することができ、例えば、仮想通信路上に複数相互のエージェント間連携の構築、エージェント間連携の分割、統合、入れ子状態のエージェント間連携の構築などが可能である。

【０１２１】

また、本発明のエージェント連携システムは、アクセス権管理、不正アクセス検知、メッセージの暗号化復号化処理を備えた構成とし、仮想通信路、エージェント間連携、メッセージ送受信に対するセキュリティを向上することができる。

【０１２２】

また、本発明のエージェント連携システムは、ポリシーを一元的に管理し、頒

布するポリシーリポジトリサーバを備え、未だポリシーを持っていないエージェントに対するポリシーの頒布を実行でき、また、ポリシーそのものの更新がある場合においてエージェントに対して更新後のポリシーを頒布することができる。

【図面の簡単な説明】

【図１】　本発明で用いるポリシー文法の一部の例を示した図

【図２】　本発明の実施形態１のエージェント連携システムの装置構成例を模式的に示す図

【図３】　本発明の実施形態１のエージェント連携システムにおける仮想通信路構築動作、エージェント連携動作例を示したフローチャート

【図４】　（ａ）が複数相互のエージェント間連携の構築の様子を概念的に示したもの、（ｂ）が複数相互のエージェント間連携を統合する様子を概念的に示したもの、（ｃ）がエージェント間連携を分割する様子を概念的に示したもの、（ｄ）がエージェント間連携の入れ子状態の様子を概念的に示したもの

【図５】　本発明の実施形態３のポリシー証明とロール保証の概念を模式的に示す図

【図６】　本発明の実施形態３のエージェント連携システムの装置構成例を模式的に示す図

【図７】　本発明の実施形態４のエージェント連携システムの装置構成例を模式的に示す図

【図８】　本実施形態５における本発明のオブジェクトエージェント連携システムを実現する処理プログラムを記録した記録媒体の例を示す図

【符号の説明】

５　ポリシー管理機関

６　属性管理機関

７　個体認証機関

８　トラストエンジン

１０　エージェントネットワークコネクタ

１１　アクセス権管理部

１２　不正アクセス検知部

２０　セキュリティマネジャ

３０　ロールマネジャ

４０　属性マネジャ

５０　ロールプログラムデータベース

６０　フィールドコネクタ

７０　ロールメソッドテーブル

８０　ロール実行部

９０　エージェント連携確認部

１００，１００ａ　エージェント

２００　外部ネットワーク

２１０　内部フィールド

３００　ポリシーリポジトリサーバ

１０００　記録装置内の記録媒体

１００１　可搬型記録媒体

１００２　ＣＤ－ＲＯＭ

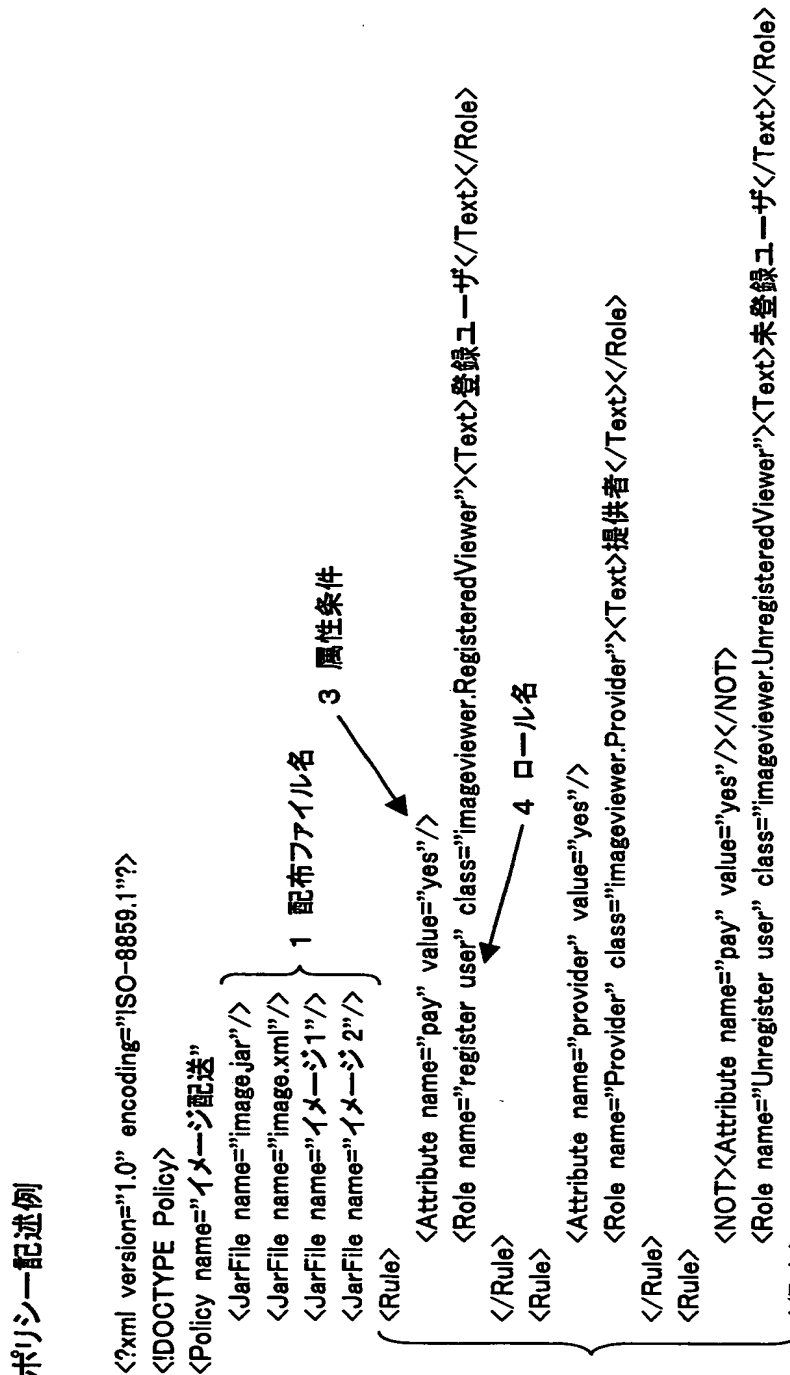
１００３　フレキシブルディスク

１００４　コンピュータ

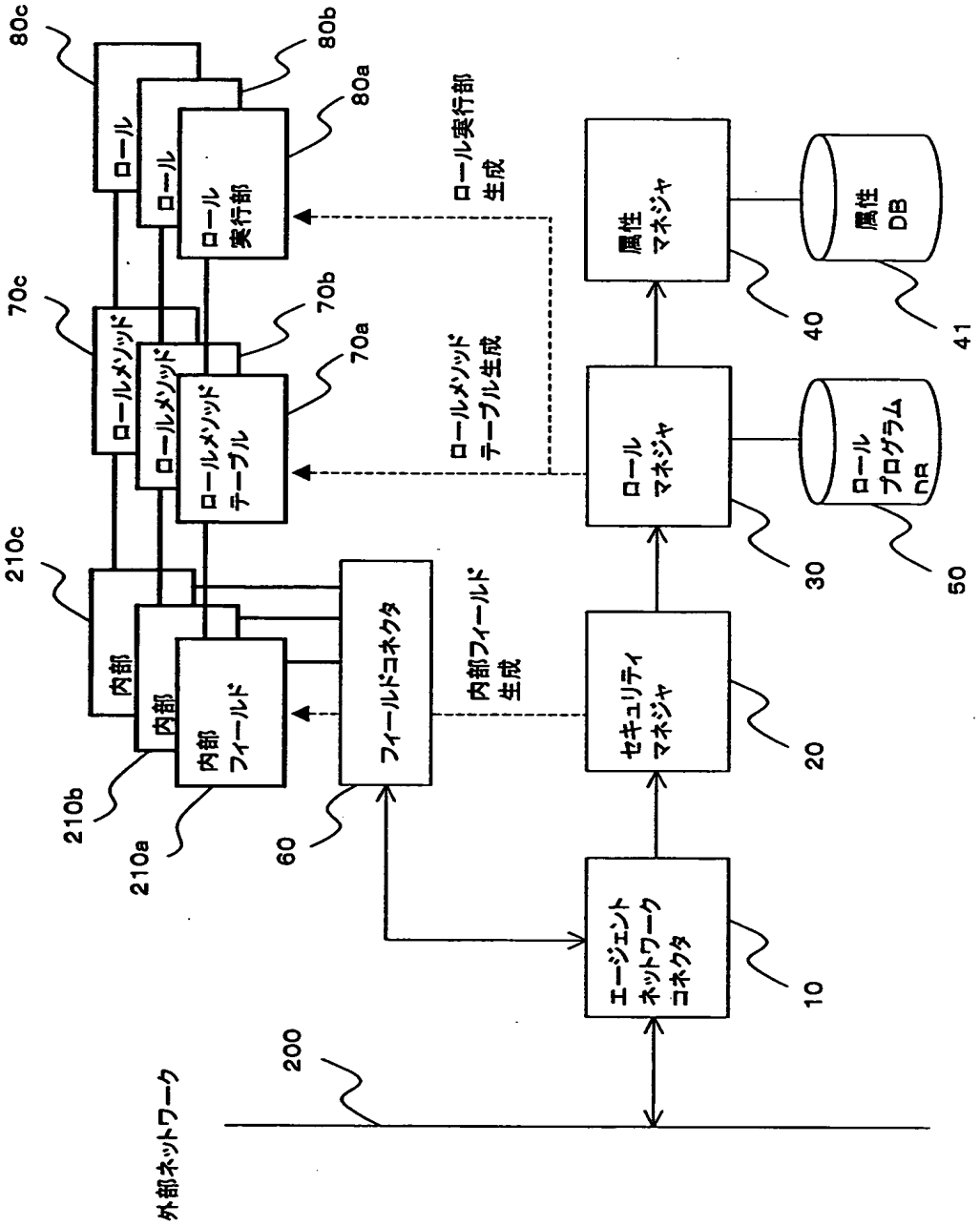
１００５　コンピュータのハードディスクやＲＡＭ等の記録媒体

【書類名】　　図面

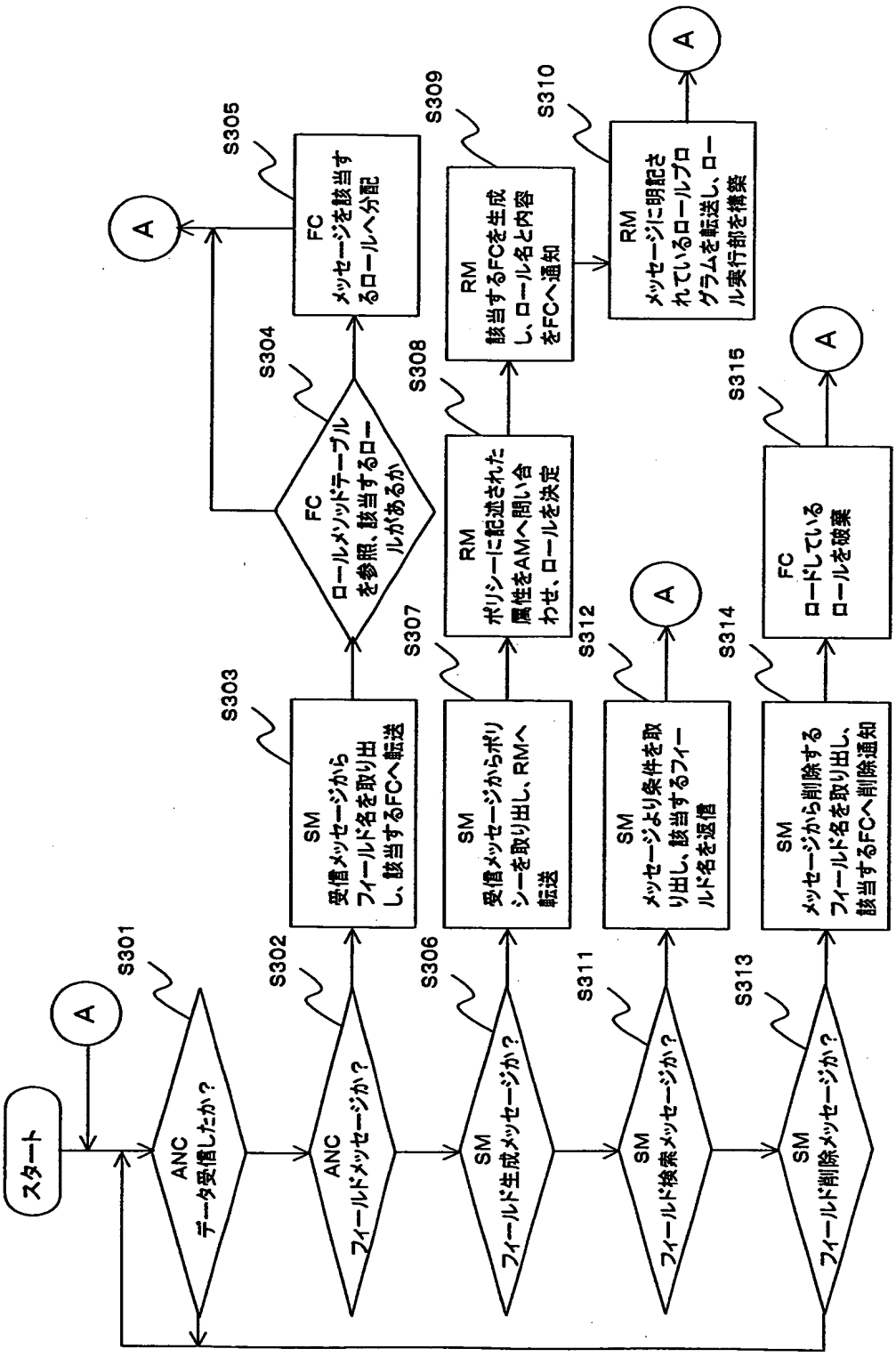
【図１】


ポリシー記述例
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE Policy>
<Policy name="イメージ配送">
<JarFile name="image.jar"/>
<JarFile name="image.xml"/>
<JarFile name="イメージ1"/>
<JarFile name="イメージ2"/>
1 配布ファイル名
<Rule>
<Attribute name="pay" value="yes"/>
3 属性条件
<Role name="register user" class="imageviewer.RegisteredViewer"><Text>登録ユーザ</Text></Role>
4 ロール名
</Rule>
<Rule>
<Attribute name="provider" value="yes"/>
<Role name="Provider" class="imageviewer.Provider"><Text>提供者</Text></Role>
</Rule>
<Rule>
<NOT><Attribute name="pay" value="yes"/></NOT>
<Role name="Unregister user" class="imageviewer.UnregisteredViewer"><Text>未登録ユーザ</Text></Role>
</Rule>
</Policy>
ルール 2

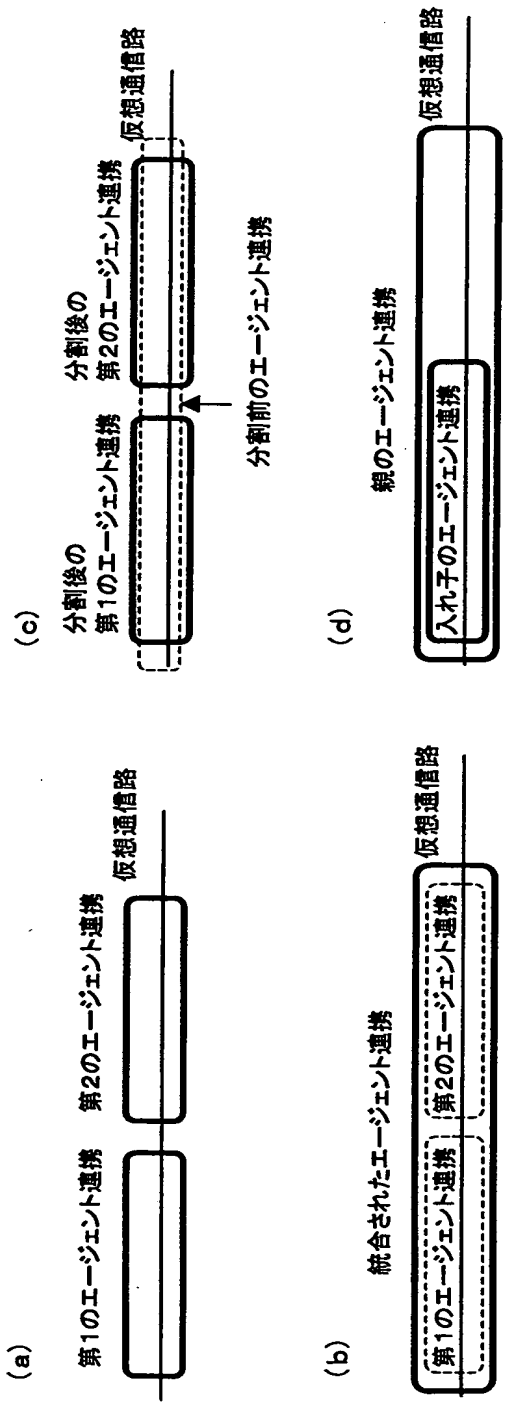
【図２】


80c
80b
80a
ロール
ロール
ロール実行部
ロール実行部生成
属性マネジャ
属性DB
40
41
70c
70b
70a
ロールメソッド
ロールメソッド
ロールメソッドテーブル
ロールメソッドテーブル生成
ロールマネジャ
ロールプログラムDB
30
50
210c
210b
210a
内部
内部
内部フィールド
フィールドコネクタ
60
内部フィールド生成
セキュリティマネジャ
20
エージェントネットワークコネクタ
10
200
外部ネットワーク

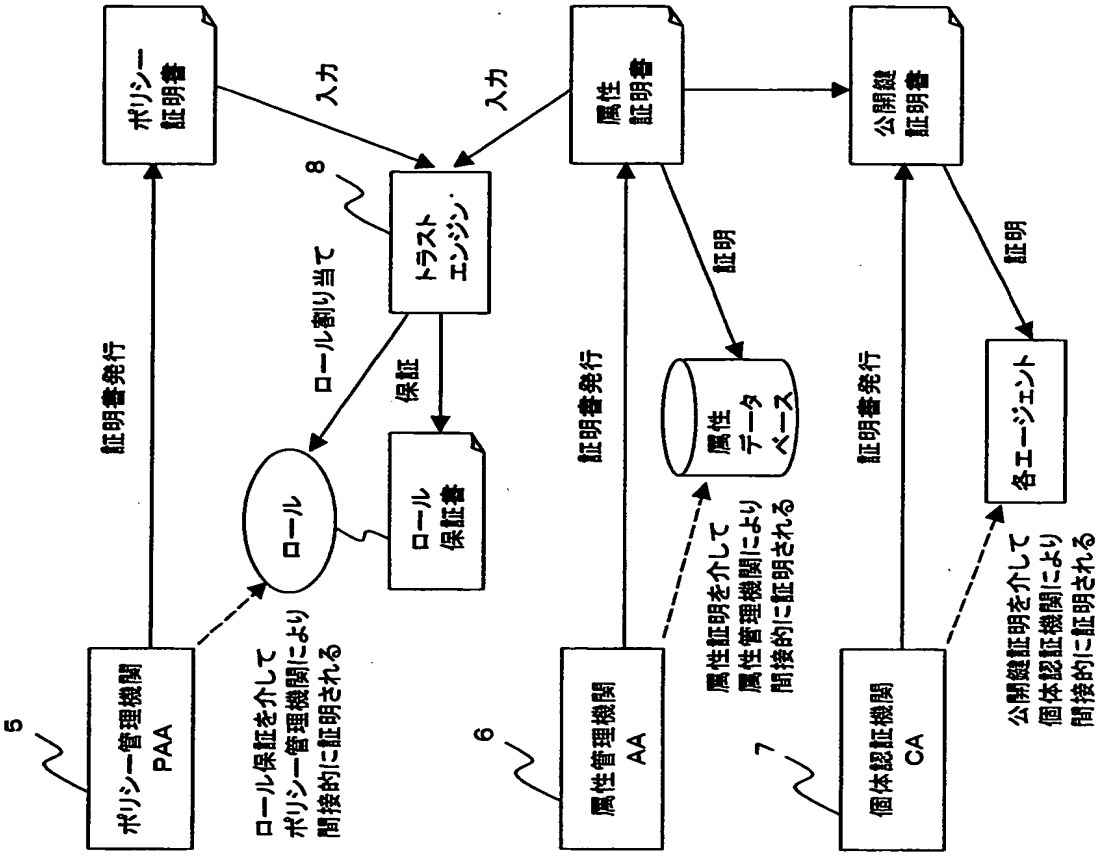
【図３】


スタート
A
S301
ANC
データ受信したか？
S302
ANC
フィールドメッセージか？
S303
SM
受信メッセージから
フィールド名を取り出
し、該当するFCへ転送
S304
FC
ロールメソッドテーブル
を参照、該当するロー
ルがあるか
S305
FC
メッセージを該当す
るロールへ分配
S306
SM
フィールド生成メッセージか？
S307
SM
受信メッセージからポリ
シーを取り出し、RMへ
転送
S308
RM
ポリシーに記述された
属性をAMへ問い合
わせ、ロールを決定
S309
RM
該当するFCを生成
し、ロール名と内容
をFCへ通知
S310
RM
メッセージに明記さ
れているロールプロ
グラムを転送し、ロー
ル実行部を構築
A
S311
SM
フィールド検索メッセージか？
S312
SM
メッセージより条件を取
り出し、該当するフィー
ルド名を返信
A
S313
SM
フィールド削除メッセージか？
S314
SM
メッセージから削除する
フィールド名を取り出し、
該当するFCへ削除通知
S315
FC
ロードしている
ロールを破棄
A

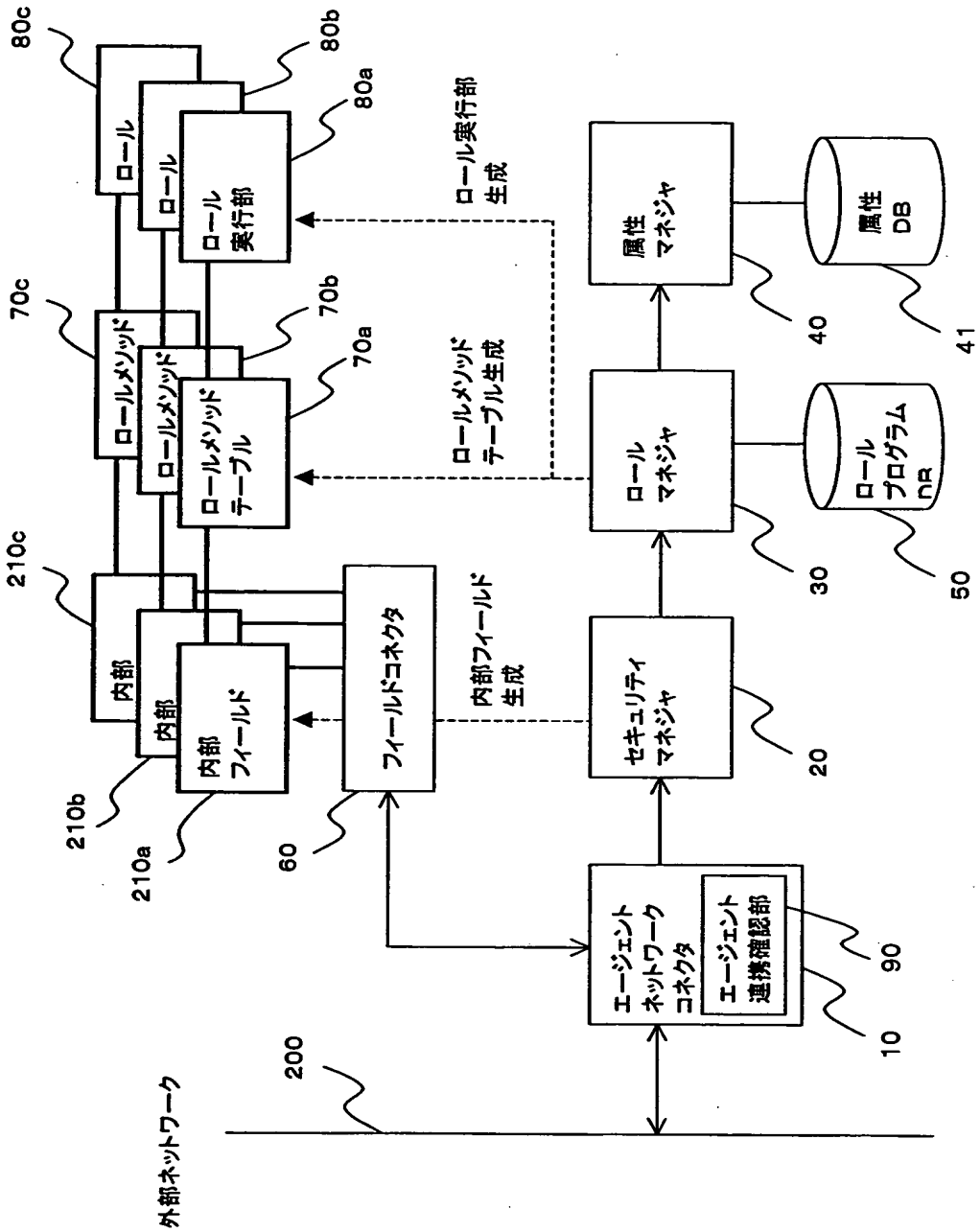
【図４】


(a)
第1のエージェント連携
第2のエージェント連携
仮想通信路
(b)
統合されたエージェント連携
第1のエージェント連携
第2のエージェント連携
仮想通信路
(c)
分割後の
第1のエージェント連携
分割後の
第2のエージェント連携
仮想通信路
分割前のエージェント連携
(d)
親のエージェント連携
入れ子のエージェント連携
仮想通信路

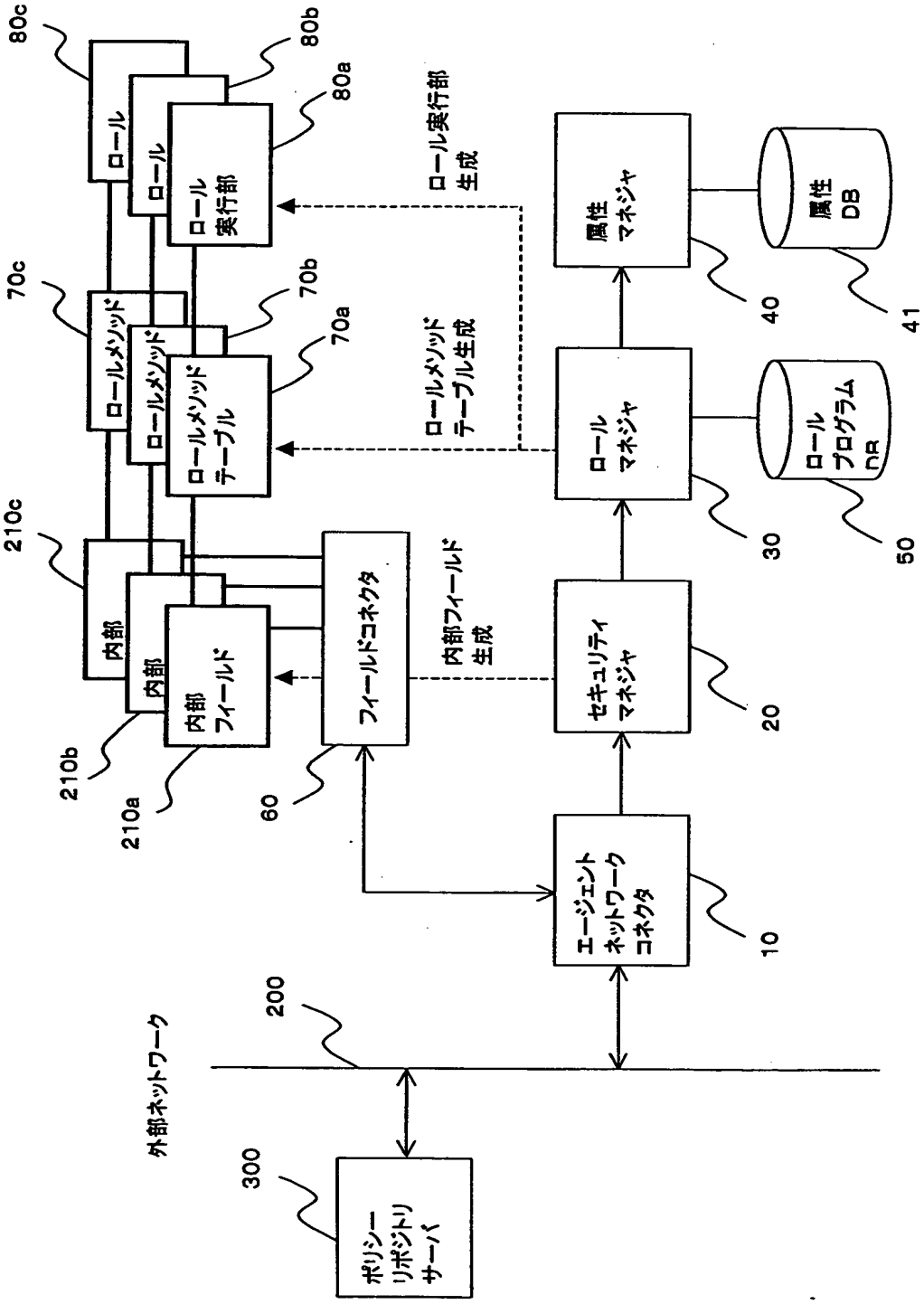
【図５】


ポリシー証明書
入力
入力
属性証明書
公開鍵証明書
8
トラストエンジン
ロール割り当て
保証
証明
証明
証明書発行
証明書発行
証明書発行
ロール
ロール保証書
属性データベース
各エージェント
5
ポリシー管理機関 PAA
6
属性管理機関 AA
7
個体認証機関 CA
ロール保証を介して ポリシー管理機関により 間接的に証明される
属性証明を介して 属性管理機関により 間接的に証明される
公開鍵証明を介して 個体認証機関により 間接的に証明される

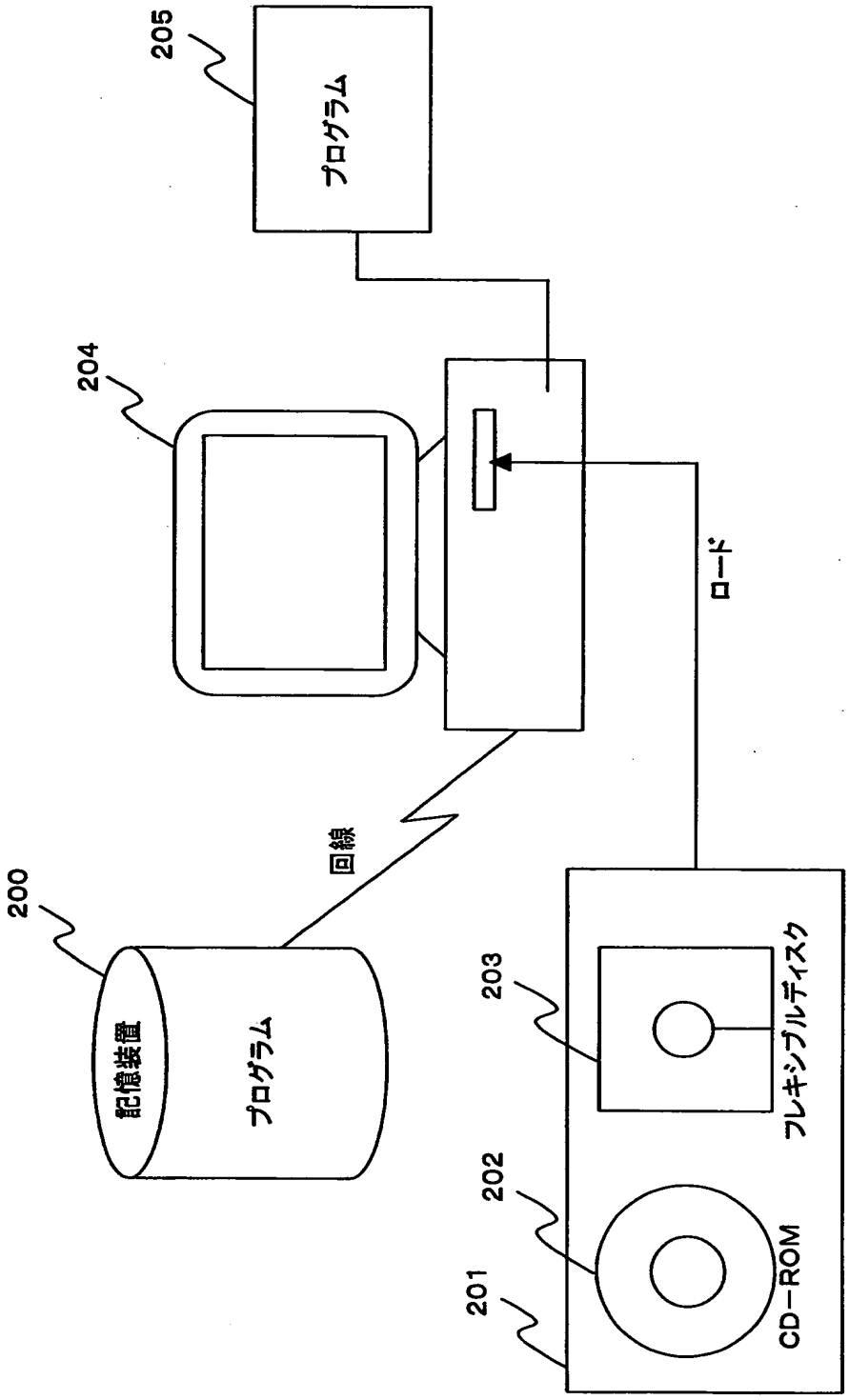
【図６】


80c
80b
80a
ロール
ロール
ロール実行部
ロール実行部生成
70c
70b
70a
ロールメソッド
ロールメソッド
ロールメソッドテーブル
ロールメソッドテーブル生成
属性マネジャ
属性DB
40
41
ロールマネジャ
ロールプログラムDB
30
50
210c
210b
210a
内部
内部
内部フィールド
フィールドコネクタ
内部フィールド生成
60
セキュリティマネジャ
20
エージェントネットワークコネクタ
エージェント連携確認部
90
10
200
外部ネットワーク

【図７】


80c
80b
80a
ロール
ロール
ロール
実行部
ロール実行部
生成
70c
70b
70a
ロールメソッド
ロールメソッド
ロールメソッド
テーブル
ロールメソッド
テーブル生成
属性
マネジャ
属性
DB
40
41
ロール
マネジャ
ロール
プログラム
DB
30
50
210c
内部
内部
フィールド
フィールドコネクタ
内部フィールド
生成
セキュリティ
マネジャ
20
210b
210a
60
エージェント
ネットワーク
コネクタ
10
200
外部ネットワーク
300
ポリシー
リポジトリ
サーバ

【図８】


205
プログラム
204
ロード
回線
200
記憶装置
プログラム
203
フレキシブルディスク
202
CD−ROM
201

【書類名】　要約書

【要約】

【課題】　要求やサービス内容に応じて情報を送受信する仮想通信路を柔軟かつ動的に構築し、エージェント間の連携を実現する。

【解決手段】　ネットワーク上の各エージェント１００に対してエージェントの属性と権限を関係づけたポリシーを頒布する。セキュリティマネジャの指示によりフィールドコネクタ６０が内部フィールド２１０を生成し、ロールマネジャ３０は、属性マネジャからの属性情報を利用し、各エージェントの属性に応じた権限（ロール）を各エージェントに与え、ロールメソッドテーブル７０、ロール実行部８０を構築する。各エージェントはメッセージを外部ネットワークから受け取るとロールメソッドテーブルを参照して該当するロールを検索し、ロール実行を行う。メッセージのやり取りを通じて仮想通信路を介したエージェント間の連携を実現する。

【選択図】　図２

出願人履歴情報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社